REMARKS

In the Official Action mailed on **06 July 2009**, the Examiner reviewed claims 1-4, 6-11, 14-17, 19-31 and 33-40. Examiner rejected claims 1-4, 6-11, 14-17, 19-31, and 33-40 under 35 U.S.C. § 103(a) based on Pruthi (U.S. Pub. No. 2004/0015581, hereinafter "Pruthi"), and Bruton et al. (U.S. Patent No. 7,222,366, hereinafter "Bruton").

Rejections under 35 U.S.C. § 103(a)

Examiner rejected claims 1-4, 6-11, 14-17, 19-31, and 33-40 under 35 U.S.C. § 103(a) based on Pruthi and Bruton. Applicant respectfully disagrees with this rejection. Neither Pruthi nor Bruton discloses aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update period, **where aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits**.

Examiner states that Pruthi discloses aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update period, citing Pruthi, Fig. 10: reference numbers 1013-1015 and pars. [0092]-[0094]. But these citations reveal that the records are "aggregated over the **time interval** entered by the operator in the start and stop field, such as 2 hours." In other words, Pruthi only discloses aggregation over time and **not** aggregation over connection habits.

Bruton discloses detection of fast and slow scanning attacks (Bruton, C8:L4-19), where the fast scanning attack is over a short interval of **time** and the slow scanning attack is over a longer interval of **time**. However, Bruton does not disclose aggregation over connection habits.

In contrast, embodiments of the present invention involve aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update period, **where aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits**. See instant application, P33:L21-30. Grouping by similar connection habits enables embodiments of the present invention to detect scanning attacks orchestrated by hosts spread over different geographic locations (see instant application, P33:L12-16). Note that such detection is not possible by aggregating host-pair connection records by time intervals only.

Neither Pruthi nor Bruton discloses **aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits.** Hence neither Pruthi nor Bruton can detect scanning attacks from hosts spread over different geographic locations.

Applicant has amended independent claims 1, 8, 14, 20, 24, 28, and 37-40 to clarify that embodiments of the present invention involve aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update period, **where aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits**. Support for these amendments is found in instant application, P33:L21-30. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1, 8, 14, 20, 24, 28, and 37-40 as presently amended are in condition for allowance. Applicant also submits that claims 2-4, 6, and 7, which depend upon claim 1, claims 9-11, which depend upon claim 8, claims 15-17 and 19, which depend upon claim 14, claims 21-23, which depend upon claim 20, claims 25-27, which depend on claim 24, claims 29-31, which depend on claim 28, and claims 34-36,

which depend upon claim 33, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By /Shun Yao/
Shun Yao
Registration No. 59,242

Date: 06 October 2009

Shun Yao
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com